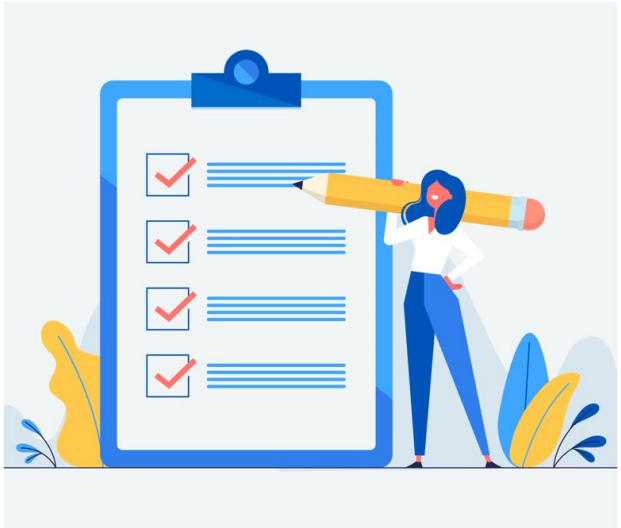
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 1

Nota : **https://revistabyte.es/ciberseguridad/ryuk-ministerio-de-trabajo/**

¿Qué tipo de amenaza es? **Ryuk** - **Ransomware**

¿Cómo comienza y cómo se propaga esta amenaza? **Ataca 1ro phishing basado en Emotec (troyano), 2do Trickbot, que se encarga del robo de credenciales de inicio de sesión, 3ro, Ryuk es el encargado de encriptar todos los datos.**

¿Hay más de una amenaza aplicada ? **Si. 3.**

¿Qué solución o medida recomendarían ? **Recomendamos utilizar el backup que debería tener el ministerio. si esto no es asi, la solucion seria perder todo o aceptar el acuerdo monetario que propone el maleante que envió ese virus.**

Mesa 2

Nota : https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/

¿Qué tipo de amenaza es? Malware Troyan backdoor

¿Cómo comienza y cómo se propaga esta amenaza?

Aprovecha la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red. Una vez dentro de un sistema, sus operadores utilizan herramientas de código abierto para escanear el entorno y realizar movimiento lateral. Tiene como objetivo los medios extraíbles para la recopilación y exfiltración de datos.

¿Hay más de una amenaza aplicada ? Troyan, spyware

¿Qué solución o medida recomendarían ?

Crear copias de seguridad en dispositivos externos y reinstalar los sistemas operativos

Mesa 3

Nota : https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/

¿Qué tipo de amenaza es? Malware, backdoor, espionaje.

¿Cómo comienza y cómo se propaga esta amenaza? El backdoor, principal componente de Vyveva, se conecta a los servidores de C&C y ejecuta los comandos emitidos por los atacantes.

¿Hay más de una amenaza aplicada ? Si. Ejecución, persistencia, evasión de defensa, descubrimiento, colección, comando y control, exfiltración.

¿Qué solución o medida recomendarían ? Descargar un antivirus.

Mesa 4

- **Nota:** https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/
- ¿Qué tipo de amenaza es? Malware.
- ¿Cómo comienza y cómo se propaga esta amenaza?
  Kobalos puede activarse mediante una conexión TCP entrante a un servicio legítimo desde un puerto de origen específico. El uso de credenciales robadas parece ser una de las formas en que se puede propagar.
- ¿Hay más de una amenaza aplicada ? Sí. Persistencia, evasión de defensa, comando y control.
- ¿Qué solución o medida recomendarían ?
  Es posible detectar Kobalos buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH. El uso de 2FA podría haber mitigado la amenaza.

Mesa 4

- Nota:https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/
- ¿Qué tipo de amenaza es? Malware.
- ¿Cómo comienza y cómo se propaga esta amenaza?
  Kobalos puede activarse mediante una conexión TCP entrante a un servicio legítimo desde un puerto de origen específico. El uso de credenciales robadas parece ser una de las formas en que se puede propagar.
  ¿Hay más de una amenaza aplicada ? Sí. Persistencia, evasión de defensa y comando y control.
- ¿Qué solución o medida recomendarían ?
  Es posible detectar Kobalos buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH. El uso de 2FA podría haber mitigado la amenaza.

Mesa 5

Nota : <Poner el link>JAJAJAJAJAJAJAAJJAAJAJJAAJJAJJAJJAJAJAJAJAJAJAJJAAJAJA

¿Qué tipo de amenaza es? **Trojan; Usando un programa que instala una vulnerabilidad en un sistema, disfrazado como un programa benigno.**

¿Cómo comienza y cómo se propaga esta amenaza?HOLAAAA

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 6

Nota : https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/

¿Qué tipo de amenaza es?

un backdoor y un troyano.

¿Cómo comienza y cómo se propaga esta amenaza?

Según nuestra telemetría, la campaña distribuyendo estas herramientas ha estado activa desde 2016, con las detecciones más recientes de julio de 2019. Los atacantes han estado distribuyendo sus herramientas a través de correos electrónicos maliciosos (“malspam”) con enlaces que conducen a un archivo malicioso.

¿Hay más de una amenaza aplicada ?

Si, hay 2 BalkanDoor y BalkanRAT.

¿Qué solución o medida recomendarían ?

Prevenir la situación por medio de capacitación para conocer más sobre el tema y evitar caer en esas trampas.

Mesa 8

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 9

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 10

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 11

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 12

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?